REMARKS

The present amendment is responsive to the final Office Action issued April 20, 2005. A Request for Continued Examination is submitted herewith. Claims 1, 11, 21 and 31 have been amended and new claims 41-44 have been added. No new matter has been added by the amendments or the new claims. Therefore, claims 1-2, 6-12, 16-22, 26-32, and 36-44 are now presented for consideration in view of the following remarks.

Claims 1-2, 6-12, 16-22, 26-32, and 36-40 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,894,516 ("*Brandenburg*"). The rejection states:

> As for the amended claim feature that the unique terminal identification information is selected in a manner that is unrelated to the authentication data, *Brandenburg* teaches that the encryption key is generated using the ID code of the terminal. However, *Slivka* [U.S. Patent No. 6,049,671], which is in the same field of endeavor, teaches transmitting software updates to a costumer [*sic*] terminal using the well-known RSA encryption scheme, (col. 9, lines 23-25 & col. 17, lines 6-25). It would have been desirable for one of ordinary skill in the art at the time the invention was made to modify Brandenburg to utilize the RSA algorithm as taught by *Slivka*, at least for the well known benefit of a more robust encryption process (1024 bit number) using a random number generator, which is more secure and less able to be cracked by a hacker.
>
> (Office Action, pg. 3.)

Applicants respectfully submit that the present invention is not anticipated by *Brandenburg* as noted in the foregoing rejection, as the Examiner acknowledges that *Brandenburg* does not include all of the limitations of independent claims 1, 11, 21 and 31. Applicants also submit that the presently claimed invention is not rendered obvious by *Brandenburg* in view of *Slivka*.

As discussed in the supplemental amendment submitted on January 7, 2005, *Brandenburg* discloses a broadcast software distribution system that can transmit data from a software distribution center ("SDC") to a target computer via a satellite link. *Brandenburg* states the "encryption key is then itself encrypted using a target computer identification code, and the encrypted encryption key is loaded onto the target computer." (Abstract.)

The *Brandenburg* system operates as follows. A user of the target computer initiates a request for a new software package stored by the SDC. (*See* col. 2, lns. 58-67.) "For each software package, an encryption key is generated and the software package is encrypted using that encryption key." (Col. 2, line 67 to col. 3, line 2.) "A customer gives his identification code to the operator receiving the software order at the SDC." (Col. 3, lns. 33-35.) Then, "When the SCD receives the identification number of the target computer 18, it produces a new key (e.g., an ASCII string) by encrypting the software encryption key for the ordered software package using the identification code of the target computer." (Col. 3, lns. 37-40, emphasis added.)

After the encrypted encryption key is sent to and stored by the target computer, the software ordered by the user is then transmitted to the target computer. "Preferably, popular products are broadcast at regular intervals, while relatively uncommon software products are periodically scheduled at the request of the user." (Col. 3, lns. 63-65.) Then, "the target computer decrypts the encrypted encryption key using its identification code. Once this is performed, the target computer decrypts the software using the encryption key specific to the software product." (Col. 4, lns. 22-26, emphasis added.) In an alternative, a receiver/installer program on the target computer "itself generates the identification code. The

receiver/installer program 14 on the target computer 18 utilizes this identification number to decrypt the encrypted encryption key. The encryption key in turn enables the target computer 8 to decrypt (i.e., unlock) the transmitted software. (Col. 4, lns. 32-37.)

Slivka "relates to a system for automatically identifying software that may be appropriate for installation on a computer and for making that software available to that computer." (Col. 1, lns. 11-24.) *Slivka* goes on to state that an "encryption scheme may also be used to permit safe transfer of the software to the user computer." (Col. 9, lns. 24-25.) The RSA encryption scheme is identified at column 17 as indicated by the Examiner.

Applicants respectfully submit that *Brandenburg* and *Slivka*, taken alone or in combination, neither disclose nor suggest each and every element of independent claims 1, 11, 21 and 31. Indeed, as demonstrated below, the Examiner's rejection should be withdrawn because the combination does not result in the claimed invention and there is no teaching, suggestion, or motivation to combine the references as proposed by the Examiner to arrive at the claimed invention.

First, the technical teachings of *Brandenburg* and *Slivka* are such that their combination would not result in the claimed invention, even if combined. *Brandenburg* neither teaches nor suggests unique terminal identification information that is selected in a manner unrelated to the authentication data. Instead, the broadcast software distribution system of *Brandenburg* encrypts its software encryption key for the ordered software package using the identification code of the target computer.

An attempt was made in the Office Action to remedy this substantial deficiency by relying on *Slivka*. As discussed above, *Slivka* discloses a system for automatically identifying

software for installation on a computer and for making that software available to the computer. While *Brandenburg* provides "a unique method, apparatus, and article of manufacture for broadcasting encrypted software to a target computer," *Slivka* does not address broadcasting of software at all. (*Brandenburg*, col. 1, lns. 57-59, emphasis added.) *Brandenburg's* encryption scheme appears tailored for the problem of broadcasting software updates. (*See* col. 1, lns. 46-51.)

In addition, *Brandenburg* does not disclose additional elements of the independent claims. By way of example only, claim 1 also requires "communicating between said one receiving terminal and the transmission apparatus via an Internet system, said one receiving terminal being operable to receive a digital broadcasting signal." Claim 11 requires "said one receiving terminal being operable to output said authentication data, to receive said unique terminal information and said update program, to communicate with said transmission apparatus via an Internet system, and to receive a digital broadcasting signal, and said one receiving terminal including a specified storage location operable to store said unique terminal information and said update program to update said processing." Claim 21 requires "a plurality of receiving terminals, one of said plurality of receiving terminals being operable to communicate with the transmission apparatus via an Internet system, to receive a digital broadcasting signal, to output authentication data associated with said one receiving terminal, and, upon authentication of said authentication data by said transmission apparatus, to receive unique terminal information identifying said one receiving terminal as a destination of transmission and an update program for changing the processing of said one receiving terminal." And claim 31 requires "communicating between said one receiving terminal and the transmission apparatus via an Internet system, said one receiving terminal

being operable to receive a digital broadcasting signal." *Slivka* also does not disclose these additional elements of the independent claims. Thus, *Slivka* cannot remedy the deficiencies of *Brandenburg*.

Thus, even if one could import the teachings of *Slivka* into *Brandenburg*, which applicants do not believe is the case, the combination would not have each and every element required by independent claims 1, 11, 21, and 31. By way of example only, the combination of *Slivka* and *Brandenburg* would not result in unique terminal identification information that is selected in a manner unrelated to authentication data.

Also, there is no teaching or suggestion as to how *Brandenburg* could be redesigned to incorporate the RSA algorithm of *Slivka* while still achieving its goals of broadcast downloading of software. As discussed above, *Brandenburg* uses the identification code of the target computer to both encrypt and decrypt the encryption key. It does not appear that the RSA algorithm mentioned by *Slivka* could simply be implemented in lieu of *Brandenburg's* recited encryption scheme. Finally, it is not even clear that such a combination is feasible based upon the broadcast system of *Brandenburg*.

Second, one skilled in the art would not have been motivated to combine the teachings of *Brandenburg* and *Slivka*. The asserted motivation supplied by the Examiner, namely a more robust encryption process, appears to be irrelevant given the broadcast system and specific teachings of *Brandenburg*. *Brandenburg* utilizes a unique computer identifier code associated with the computer to both encrypt and decrypt an encryption key, which teaches away from using a random number generator as suggested by the Examiner. *Slivka* utilizes the RSA encryption algorithm to safely transfer software to a user's computer. It is not clear or obvious to use the RSA algorithm in broadcast download of software to multiple terminals, such as

in a satellite set top box system. Rather, the teachings of *Slivka* go against the teachings of *Brandenburg*.

The fact that a prior art process or device could be modified so as to produce the claimed invention is not a basis for an obviousness rejection unless the prior art suggests the desirability of such modification. *In re Gordon*, 733 F.2d 900, 221 U.S.P.Q. 1125 (Fed. Cir. 1984). As stated in *In re Oetiker*, 997 F.2d 1443, 1447, 24 U.S.P.Q.2d 1443 (Fed. Cir. 1992):

> There must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the field of the invention would make the combination. That knowledge cannot come from the applicant's invention itself.

There is simply no teaching or motivation in the cited art to reengineer the *Brandenburg* system using an incompatible encryption scheme as disclose in *Slivka* in order to arrive at the elements recited in claims 1, 11, 21 and 31.

In view of the foregoing, it is respectfully submitted that claims 1, 11, 21 and 31 patentably distinguishes over *Brandenburg* and *Slivka*, both individually and in the combination that the Examiner suggests can be made therefrom. Therefore, applicants respectfully request reconsideration and allowance of the claims.

Furthermore, claims 2, 6-10, 12, 16-20, 22, 26-30, 32, and 36-44 depend from independent claims 1, 11, 21 and 31, respectively, and contain all of the limitations thereof as well as other limitations that are neither disclosed nor suggested by the prior art of record. Accordingly, applicants submit that the subject dependent claims are likewise patentable.

In addition to the reasons presented above, new claims 41-44, which depend from independent claims 1, 11, 21 and 31, respectively, are also patentable in that they each require that either the unique terminal identification information or the unique terminal information "comprises a MAC address of said one

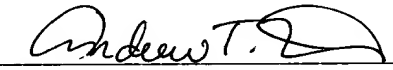
receiving terminal." Neither *Brandenburg* nor *Slivka* teaches or suggests, either alone or in combination, the limitations of claims 41-44. Accordingly, applicants submit that dependent claims 41-44 are patentable as well.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of the claims and to pass this application to issue. If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he telephone applicants' attorney at (908) 654-5000 in order to overcome any additional objections which he might have.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: July 20, 2005

Respectfully submitted,

By 

Andrew T. Zidel
Registration No.: 45,256
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicant

580925_1.DOC